National Security Agency

General Keith Alexander Speaks at AFCEA's Conference

Speaker:
General Keith Alexander,
Director, National Security Agency
and Commander, U.S. Cyber Command

Location:
Baltimore Convention Center,
Baltimore, Maryland

Time: 1:00 p.m. EDT
Date: Thursday, June 28, 2013

Transcript by
Federal News Service
Washington, D.C.

GENERAL KEITH ALEXANDER: Can we turn (up ?) the lights? (Laughter.) So, you know, when I go home with a suntan today, my wife is going to say, so where were you? And I say, well, I had a few briefings down on the Hill and then up here. And you've got a burn. I can see – (inaudible). Hey, Charlie. Good to see you.

OK. Chaplain, let's give the chaplain a great round of applause. That was absolutely superb. (Applause.) So you know, as you were doing that, I'm thinking, I've got my four daughters, their husbands and 15 grandchildren coming in over the next several days. And when you talked about Gettysburg, I thought you were talking about them assaulting our house. It is.

Well, one, thanks for putting this on and to FC (ph). I think this has been a great opportunity to discuss some key issues for cyber. I think some of the stuff that we talked about in terms of interoperability, command and control, collaboration, the joint information environment, securing, operating and defending our networks, workforce developments in our times and cybersecurity awareness and education – absolutely superb. And for the teachers that are here, thanks. Thanks for what you're doing to help bring along the youth of America. Let's give them a big round of applause, folks. (Applause.)

Before I go into my cyber discussion, I thought it was important for me to address some of the media leaks that are going on, and I think it's important that you hear from me some of this. I want to make six key points.

First, our responsibility, my main responsibility is defense of this country. These programs are part of that effort. In 2001, after 9/11, it was determined by the 9/11 Commission that the intelligence community could not connect the dots, foreign and domestic. We set about as a community to figure out how could we connect those dots. What programs do we need? And how do we do this under a legal framework? And we set up these two programs, 215, Section 215 for the business records FISA, and 702, as two of the capabilities look at a methodology to help us connect those dots. These capabilities were approved by the administration – thank you – Congress and the FISA court. With these exceptional authorities came equally exceptional oversight by all three branches of the government. These programs are focused with distinct purposes and oversight mechanisms. We understand and support the need to ensure we protect both civil liberties and national security. It's not one or the other. It must be both. That's why we take oversight of these programs very seriously.

A report issued by the Senate Select Intelligence Committee in June 2012, in support of the reauthorization of the 2008 amendments to FISA, emphasized that the government implements this authority in a responsible manner. And I quote: "Through four year of oversight, the committee has not identified a single case in which a government official engaged in willful effort to circumvent or violate the law – not one case in four years."

I'd like to just give you some insights on the business record FISA first and use an analogy using a lockbox. Under the business record FISA, or Section 215, we take the metadata from the service providers and place it into a virtual lockbox. The only way NSA can go into that lockbox is if we have what is called reasonable, articulable suspicion of a selector that is related to terrorism. In all of 2012, we approved less than 300 selectors – such as telephone numbers – to initiate queries into that virtual lockbox. There has to be a foreign nexus, an association with al-Qaida or other specified terrorist organizations.

Operation High Rise is a great case in point. Now I won't give this as good as the deputy director of the FBI, Sean Joyce, did in our open hearing before the House last week, but I think it's important just to discuss this one, and then the others you can look at that open testimony and see what Sean actually said.

But just to review for you, Op High Rise: NSA was tracking terrorists in Pakistan. We used FAA 702 to get their email. We compelled that service provider to get us that email under a court order, that FAA 702. With that, armed with that information, we found that they were – this guy in Pakistan, an al-Qaida terrorist, was talking to a guy on email we believed to be in Colorado. We gave that to the FBI. That's our job: helping to connect the dots. In that, there was a telephone number that the FBI came up and said, hey, this is Najibullah Zazi, and we are concerned about this. We then used the business record FISA to go look in that virtual lockbox. We took that number, we got reasonable, articulable suspicion and we looked in that lockbox, and we found that Zazi was talking to a guy in New York who had connections to other terrorist elements for another operation on the second plot and others on a third plot. That information, along with information – the Customs and Border Patrol, CIA and our entire community brings together helped FBI stop that plot. We got that information in early September 2009 for an attack that was supposed to take place in mid-September. It would have been the biggest al-Qaida attack on American soil since 9/11. We were privileged and honored to be a part of disrupting that plot. FAA 702 was the initial tip. That's how important these programs are.

My third point: These programs have helped us connect the dots, as I've just used in Op High Rise, but our allies have benefited, too. On 21 June, last week, last Friday, we provided 54 cases to several congressional committees in which these programs contributed to our understanding, and in many cases, helped enable the disruption of terrorist plots in the U.S. and in over 20 countries throughout the world. It is important to note we are part of a larger government that includes our great partners at FBI, CIA, DHS, the Defense Department, as well as many others. We also partner with our allies in combatting terrorism. Here are some statistics of those 54 events.

Of the 54, 42 involved disruptive plots – disrupted plots. Twelve involved cases of material support to terrorism. Fifty of the 54 cases led to arrests or detentions. Our allies benefited, too. Twenty-five of these events occurred in Europe, 11 in Asia and five in Africa. Thirteen events had a homeland nexus. In 12 of those events, Section 215 contributed to our overall understanding and help to the FBI – twelve of the 13. That's only with a business record FISA can play. In 53 out of 54 events, Section 702 data played a role, and in many of these cases, provided the initial tip that helped unravel the threat stream. A significant portion, almost half of our counterterror reporting, comes from Section 702.

Fourth, these programs operate under a rigorous oversight framework from all three branches of our government. FISA provides that in order to target the content of a U.S. persons communications anywhere in the world, NSA and the rest of our government requires a finding of probable cause under a specific court order. This translates into significant information on – these capabilities translate into significant information on ongoing terrorist activities with no willful violations of our law.

Fifty-four terrorist activities disrupted; zero willful violations. When you think about how our government operates and what we've done to bring all three branches together, I think that's something to be proud of. We have defended the nation 54 times, and our allies, and we have ensured the protection of our civil liberties and privacy in oversight by all three forms of our – all three branches of our government. I think that's what the nation expects our government to do, disrupt terrorist activities, defend our civil liberties and privacy.

Most nations around the world are capable and do collect signals intelligence, just like we do. And their governments use lawful intercept efforts that require and compel companies to provide the requested information. I think our nation is among the best at protecting our privacy and civil liberties.

And I'll just give you an aside: When President Obama came into office, I met with him in the first few weeks on these programs. And he wanted to make sure that they were essential for defending the nation and that we could, with these, still protect our civil liberties and privacy, and he pushed us in that. Along with Congress, we came up with additional measures and for NSA, we built out of those meetings our directorate of compliance to make another step in ensuring we're doing this exactly right.

Sixth, my sixth point – I'm getting through this, bear with me – public discussion of NSA's tradecraft or the tools that support its operation provides insights that our adversaries, to include terrorists, can and do use to hide their activities. Those who wish us harm now know how we counter their actions.

These leaks have caused significant and irreversible damage to our nation's security. Historically, every time a capability is revealed, we lose our ability to track those targets. What is going on in these leaks is unconscionable, in my opinion, and it hurts our nation and our allies and it's flat wrong.

There are lawful and legitimate mechanisms to raise concerns about these programs. NSA, DOD and DNI all have whistle-blower programs and investigator generals who are in a position to do this. An individual acting nobly would have chosen one of those as a course of action to reveal his concerns.

I worry that there will be more leaks and that they will attempt to further sensationalize this issue. I'd ask you to remember that context matters, that these authorities are carefully debated and considered across three branches of government and that we only employ these capabilities that we believe are both useful and necessary.

As you may have read in the media, NSA previously had an email metadata program analogous to the telephony program that has been the subject of some of this recent discussion. This program was conducted under a different provision of the Patriot Act. As has already been noted by senior officials in public comments recently, this program was terminated in 2011, because it didn't have the operational impact that we needed. That was a choice that came from us, from NSA; we started that debate and said, this did not have the value to stop the terrorist attacks that we need. We went forward to the administration and Congress and with all their support, shut that program down because it wasn't meeting what we needed and we thought we could better protect civil liberties and privacy by doing away with it, and all that data was purged at that time.

So what does that come to? A conclusion: First, the damage is real. I believe the irresponsible release of classified information about these programs will have a long-term detrimental impact on the intelligence community's ability to detect future attacks. These leaks have inflamed and sensationalized for ignoble purposes the work the intelligent (sic) community does lawfully under strict oversight and compliance.

If you want to know who's acting nobly, look at the folks at NSA, FBI, CIA and the Defense Department that defend our nation every day and do it legally and protect our civil liberties and privacy. They take an oath to our Constitution to uphold and defend that Constitution. And they take that oath seriously and they do a great job. They're the heroes that our nation should be looking at. They're the ones that are taking care of us and they're the ones protecting our civil liberties and privacy.

So that's all I wanted to say on the leaks. (Applause.)

Now for my 45-minute speech on cyber. (Laughter.) I do think it's important to put that on the table, because as we go into cyber and look at – for cyber in the future, we've got to have this debate with our country. How are we going to protect the nation in cyberspace? And I think this is a debate that we can do more transparently than we can on the counterterrorism. And it is a debate that is going to have all the key elements of the executive branch – that's DHS, FBI, DOD, Cyber Command, NSA and other partners – with our allies and with industry. We've got to figure how we're going to work together.

Now, you had some great discussion today about some of the key things, I'm going to come back and hit on those. But first, let's look at what's going on. In August of 2012, we saw that Saudi ARAMCO was hit with a destructive attack. The data on over 30,000 systems was destroyed.

In September, DDoS attacks began against our financial sector and a few hundred have gone on since then. Disruptive attacks: We saw in March of 2013 destructive attacks against South Korea. If you look at the statistics in what's going on, we're seeing an increase in the disruptive and destructive attacks, and I am concerned that those will continue and that as a nation, we must be ready.

It is a great honor and privilege in this area to partner with folks like Secretary Napolitano from DHS and Director Bob Mueller from the FBI. We each have a role. Cyber Command's role is to defend the nation. Just as the Defense Department does in other areas, our job is to defend the nation. NSA has the foreign intelligence responsibility, find out who it is, get the attribution, support DOD, DHS and FBI. That's how our team is organized.

What's happened in this space over the last several years is a convergence, and as you look at what used to be analog and digital back when Steve and I were on the Army staff – now, Steve knows I was the true G3, because you heard it up here – when we were on the Army staff, you had analog and digital traveling in different pipes, but look what's happened over the last eight years. These networks have converged. It's all digital. Our information travels on that network. Ironically, so do terrorists, so do our adversaries and so does malicious software.

And I think one of the great things – you know, I mentioned I have 15 grandchildren – they are wonderful, it really is. For one, you can hand them back – (laughter) – it's amazing. You know, I – one of them is a two-year-old – was a two-year-old boy and he got a hold of my daughter's iPad. And he was walking around and he Skyped my daughter. He was in Dallas, Texas, got that, Skyped my wife in Maryland. And he was walking around the house talking to her, and my wife said, where's your mom? Oh, she's upstairs. And so he walks up the stairs, you know, (bouncy, bounce ?) – two years old, and they can Skype. Think of how great this is for collaboration. Think about what we'll have with these systems. Look at what the mobile devices have right now – just about everybody in this audience has an iPhone or an Android or – some of us have BlackBerrys. (Laughter.) All good, all good, don't get me wrong – (laughter) – phew, that was close. (Laughter.) Exponential rates of change, right? This is going on. This is what our nation faces. It's wonderful. These capabilities, I think, are going to help us solve cancer. This is a wonderful opportunity. And for what the teachers are doing – just think how much better we can educate the next generations – absolutely superb.

But there are issues with this. We have vulnerabilities. We're being attacked. And we've got to figure out how to fix that. So here's some thoughts. First, we talked about the joint information environment. And I know that came up several times. We need to push that hard. That is a key part of a defensible architecture. And I think that is key to our future. And it helps connect, in that defensible architecture, our mobile devices with our fixed infrastructure, and do it in a better way that allows us to audit and take care of our data much better than we've done in the legacy systems. There are some huge advantages there.

Second big thing I would push, we got to train and educate our force – this is one of the biggest issues for Cyber Command – to the next level. They have to be world class. That is a great reason for having NSA and Cyber Command co-located. We can leverage the exceptional talent that the people at NSA have to help build that force. And that's superb. In fact, you know, Charlie (sp) was there – I was just talking to him – I got a class on factoring numbers. You know, this is really neat. I know all of you want that class. We'll get it to you. No, I'm just kidding.

But when you think about it, the knowledge that they have about the computers and how these work, the math that goes into it, how information systems, how computers are built, all this stuff – we need our forces at that level. And I think the training that is ongoing right now with the services that, thanks to what you and Army cyber and the rest of the team are doing, is absolutely superb.

So sequestration will create some challenges. And I think you've heard from that. It's going to impact Cyber Command and NSA. And these are things that we're going to have to work our way through. But the key things that I would push and leave you with – first, sprint to JIE. We got to create one joint integrated cyber force. And thanks to the services for the great work that you're doing on that, absolutely superb. The service chiefs and everybody are pushing to get those forces trained.

We're focusing on phase zero, how can we prevent conflict? I think that's exactly what our nation wants us to do. Great work there. One of the things – and you saw the award that came up here on the common operational picture, how do you see cyberspace? How do you solve that is a key area, of course. And finally, I think leveraging that global cryptologic platform and the alliance with industry and our allies is going to be absolutely important. How do we work together for the future of our nation?

So thanks. Thank you very much for this opportunity. I guess I'm going to take two questions. No, I don't know how many questions. No questions?

MODERATOR: Yes, sir. (Laughter.) Your first question from the audience is: What can the private sector do to best serve or support the efforts of government, DOD and civilian cybersecurity issues?

GEN. ALEXANDER: Well, there's so many. It's like Christmas; what can you do? Well, I think the most important thing, first, if we're going to have a debate on how we're going to come up with a defensible architecture and how government and industry works together, we've got to have a surge on educating the American people, Congress, the executive branch and others, how does this work? How do these things work?

We've got to take the sensationalism and the inflammatory remarks out there and give people the facts. So from my perspective, we need to move forward, I think, in cyber legislation and things like that, but what industry can do is help inform that debate. I think that's the first most important.

The second, industry owns and operates 90-plus percent of these networks. We've got to have the partnership if we're going to defend them. And we've got to come up with a partnership that the American people are comfortable with, that they know that we're protecting them and not reading their emails or listening to their calls. They know that we're doing this right and we have all the right supervision on it.

And I think those are probably the most important things that I can think of right now. One other I would add is, you know, finding adversaries and malicious software in our networks, the antivirus community and many of the companies that we have that work with us are the ones that are going to help find that. We've got have a way of pooling that information together for the common good.

MODERATOR: Thank you. Is there any idea how soon organizations within government will be able to hire cyber-qualified government employees? Do you consider lack of sufficient training resources to be a limiting factor?

GEN. ALEXANDER: My understanding is we're hiring right now. We're building the teams. We're moving out. So that's already ongoing. In fact, our intent is to build, train and field one-third of the force by the end of this fiscal year – 30 September. And we're essentially on course to do that amongst the services. So great effort there. And they're going to continue to push it.

MODERATOR: Thank you. Does the JIE construct include interoperability for coalition forces? And if so, how?

GEN. ALEXANDER: Great question. No, no, let me answer that. (Laughter.) So I think the key thing is – you know, without getting too technical, let me lay out how a cloud architecture would work. So if you think about a cloud architecture where every data element is tagged at the data element level, what you can do with the cloud architecture is give each person who's entering in a key that gives them access only to their portion of the network. And everything else is heavily encrypted and only broken by a key.

So there's one way to do it. I think that's going to take time to get to that. The second part would be, given that people will be uncomfortable with that, you can actually now give a cloud to the coalition where our data and theirs can flow over one day – or one-way pipes. I think this will be huge in moving forward.

You know, we have a tremendous alliance in Afghanistan where many nations come together for the common good. So having those common pipes – and I know Steve Butell (sp) over there can probably answer this better so I'll get a – I'll go down afterwards. But having those common pipes is essential for the future. So that's a great question, thanks.

MODERATOR: Thank you. The next question is: How is the NSA workforce dealing with the allegations and speculations in the press?

GEN. ALEXANDER: Well, I think that's one of the reasons that I wanted to talk about the media leaks. You know, I think what happens is the press gets the inflammatory and oftentimes the sensational parts. My job is it to let you know what an incredible workforce we have. They take it hard, to be real candid. Here are people whose everyday thought is defense of our country and protecting our civil liberties and privacy. They're some of the best people we have in this country.

When I think about noble people, that's who I think of. And so the reason I took time at the beginning of this is to let you know that these are great people doing great things for our country. Fifty-four terrorist plots and activities around the world, they helped stop. Zero willful violations or attempts to circumvent that law. I think that's incredible. And they are the true heroes. And along with – you know, I don't want to minimize it, because FBI's great too, CIA and others – Defense Department. It's a great team. So thanks for that question.

MODERATOR: Thank you, sir. Doctrine provides that foundational guidance for conducting military operations. What is the current status and future efforts in the development of cyber operations doctrine?

GEN. ALEXANDER: Well, we have a draft copy working through right now at Cyber Command. We've had a team working that and it's going out for comments. So how long do comments take in a bureaucracy? We should have that out in about four years. (Laughter.) I don't know how long that'll take, but we are working on it. I think that's important.

The Defense Department has already put out some doctrine – some classified doctrine about cyberspace operations. And unfortunately, some of that was leaked on the president's decisions. And so I think you see the administration is working hard to stay up on this and, I think, doing a great job.

MODERATOR: Thank you. Do you see the evolution of a separate U.S. cyber force in the future of the DOD and – I'm sorry – DHS?

GEN. ALEXANDER: Could you ask that again?

MODERATOR: Absolutely. Do you see the evolution of a separate U.S. cyber force in the future for the DOD and DHS?

GEN. ALEXANDER: I don't right now. I don't know that I would separate out the force like that. And the reason is, for the Defense Department – let me take what I'm really comfortable talking about – for the Defense Department, I think having our cyber forces connected to the services – especially those who could be doing tactical operations, is absolutely vital. If we break that connection, how do we connect them to those operational forces? That's the first step, because cyber effects will be both local, operational and strategic. So the force has to work together like that, but I do believe we need the connection to the services.

We have to have a great partnership with DHS as well. We put a team down at DHS; NSA has sent a team of about 25 people, I think, right now, that are at DHS to help them. This is something that I think we need to take a step as we've done in creating a subunified command – perhaps take another step, look at what the next step is. And each time we take a step, stand back, re-evaluate and see if there's more to go. And I think that's probably the best approach that I can see from where I stand today.

MODERATOR: Thank you. Are efforts being made to support the sharing of information with uncleared private consulting firms who support critical infrastructure and corporate cybersecurity?

GEN. ALEXANDER: So this is part of the issue is, how do you share data? I mean, this goes right back to the heart of leaks and everything else. How do you share data that is essential for protecting us in such a way that the bad guys don't get it? If we had an easy way of doing this, we could really fix any civil liberties and privacy concerns. So if you think on the leaks side of it – let's start with that. Terrorists use the same communications that we do. They are – or some of them, act in our country and in other countries. They walk among us. They use our capabilities. They're very difficult to distinguish.

In cyberspace, these tools are very similar – the malicious software. How do you find that? And once you find it, if we tell the adversary, we see this, they can change it, and we will lose it. So we've got to figure out the correct way of working with industry. And I think that's one of the issues that we're got to have that discussion with. I think Congress and the administration have done a great job in informing that discussion, and that's partly where we are in moving that cyber legislation. Thanks.

MODERATOR: Thank you. What would be the challenges for Cyber Command if our adversaries adopted a JIE-like strategy?

GEN. ALEXANDER: Hmm. It'd be more difficult. (Laughter.) So we'd ask them not to do that. (Laughter.) Is that good? (Laughter.)

MODERATOR: It's going to have to be. Thank you. (Laughter.)

The president has talked about welcoming a debate regarding privacy and national security. How do you view your ability to balance transparency and protection of capabilities that NSA needs to be successful?

GEN. ALEXANDER: Well, on this issue here, I think everyone I've talked to from the president and Congress – they've asked us to first, defend the nation – ensure what you're doing defends this country – and we want you to do everything you can to protect civil liberties and privacy and take every step. And where at all possible, be transparent so that the American people know what we're doing is exactly right. We've gotten that from the president on down, and that's what we're trying to do.

Everyone also understands, though, that if we give up a capability that is critical to the defense of this nation, people will die. And so we're very careful about how we do that. And that's the subject of where we have a responsibility to help inform that debate for the policymakers. And from my perspective, I think America would be proud to see how that is done. It's been absolutely superb, and a privilege and honor to participate in it.

MODERATOR: Thank you. Last year, you spoke about, wire speed needs to be accounted for in operations. When will this translate to acquisitions and information assurance?

GEN. ALEXANDER: I didn't get the first part. Could you say that again?

MODERATOR: Yes, sir. Last year, you spoke about wire speed needs to be accounted for in operations. Do you know when this will be translated into acquisitions?

GEN. ALEXANDER: I'm not sure I understand "wire speed." Is that 3x10^8 meters per second? (Laughter.) Or is that light speed? I'm not sure I understand the question to answer it. I hate to be that ignorant. But "wire speed" – can anyone help me on that one?

MODERATOR: Actually, what we can do is – I'll send a note back to the person that sent that in, and I will get back to you on that one. Thank you.

GEN. ALEXANDER: Please don't capture that on camera. I feel like the Great Carnac. (Laughter.) The answer is six.

MODERATOR: I think part of the problem is that people are texting in, and we're getting bits and pieces and information that's not quite what it would be if they were able to ask them live. So I think it might be the translator here; I apologize.

So the next question is, how is the NSA work force – I'm sorry –

GEN. ALEXANDER: Same answer as before. (Laughter.)

MODERATOR: Yes. The leaks have been pretty devastating. What is NSA doing to prevent it from happening again?

GEN. ALEXANDER: So there's a couple of things. There's clearly actions that we're taking to prevent a future leak, and we've taken that right off the get-go in terms of protecting our networks – all the things that you would expect us to do, we're doing, and more. And we're also supporting the Federal Bureau of Investigation – the FBI in their investigation. So I don't want to get out in front of them. We do support that. Once those two are done, we'll look at what happened, how it happened, and have we taken all the appropriate actions to fix it, and look at, who are the people that were involved. And I don't want to go beyond that, just to tell you that we're doing this exactly right.

MODERATOR: Thank you. The next question is, when do you foresee U.S. CYBERCOM getting its own acquisition and contracting organization like DITKA (ph) or DISA – like – I'm sorry – DITCO for DISA?

GEN. ALEXANDER: For DISA? I don't know. We've discussed that. So I think that is currently something that we've discussed with the other combatant commanders – the service chiefs, the secretary, but it is not on a clear path to do those. Those are things that are being considered, and I think that will be part of that deliberate, stepwise process that I referred to earlier.

MODERATOR: Sir, is there something you would like to say to the contractors that support NSA?

GEN. ALEXANDER: Yes. (Laughter.) You know, I think – from my perspective – I've been there at eight years – for eight years – almost eight years. I don't want to exaggerate; another month it'll be eight years. And we couldn't our job without the (contracting ?) the support we get from industry. It's been absolutely superb. One individual has betrayed our trust and confidence, and that shouldn't be a reflection on everybody else. There is work that we have to do to ensure that this can never happen again. That's my job. We'll take that and we'll do it very seriously.

But we need to partner with industry – NSA and Cyber Command. That's the way this full cyber area is. It is not something we can just walk away or say that we'll do ourselves. We don't' have all the talent, we don't have all the access, and we need to partner. We need to do it right, and where possible, we need to be completely transparent with the American people so that they know we’re doing it right so that we can defend our nation and our civil liberties and privacy.

So for the contractors – for all the rest of the 99.69 (out ?) that have done it right every step of the way, thanks. Thanks for your great work, and thanks for what you do.

Thank you, folks. (Applause.)

(END)